

REMARKS

In response to the Office Action mailed on August 24, 2006, Applicant respectfully requests reconsideration. Claims 1-66 were previously pending in this application. By this response, claims 1-5, 9, 10, 13, 14, 17, 20, 23, 24, 27, 30, 32-36, 40, 41, 44-46, 48, 51, 54-58, 61, 62, 65 and 66 are amended. As a result, claims 1-66 are pending for examination with claims 1, 23, 27, 32, 57 and 62 being independent.

Applicant notes with appreciation the Examiner's courtesy in conducting the telephone conference on December 11, 2006, the substance of which is summarized below in connection with the outstanding rejections.

I. Rejections Under 35 U.S.C. §112

The Office Action rejects claims 1-66 under 35 U.S.C. §112, first paragraph, as allegedly being based on a disclosure which is not enabling. The Examiner appears to present two separate basis for the rejection under 35 U.S.C. §112. First, the Office Action asserts that actions critical or essential to the practice of the invention are not included in the claims. Second, the Office Action asserts that the language "physical connection through the network" is open to several interpretations. During the telephone conference, the Examiner discussed the latter basis, indicating that he rejected the claims under 35 U.S.C. §112 because the several ways in which the above quoted language can be interpreted leaves the scope of the claims unclear. Both bases for the rejection are addressed below. Initially, however, Applicant points out that, while not agreeing with the rejection under §112, each of the independent claims have been amended to address the Examiner's concern.

During the telephone conference, Applicant's representatives explained that embodiments of the invention are directed to securing against situations in which a first host device, connected via a network to a shared resource, spoofs its identity by assuming the identity of a second host device to gain the access permissions of the second host device. Several embodiments pertaining to this type of security measure are described in detail at page 18, line 3 – page 22, line 14 of Applicant's specification. One embodiment that secures against spoofing derives from Applicant's recognition that a host device using another host device's identity will access the shared resource through a

different physical connection through the network. That is, since the two host devices are connected at different locations on the network, the network path between the two host devices will be different.

Thus, by “determining whether the one of the plurality of devices is attempting to access the shared resource through a physical connection through the network that is different than a first physical connection through the network used by the first device to access the shared resource (which is the claim language rejected on page 7, item 3 of the Office Action),” security breaches resulting from spoofing may be avoided. That is, by determining whether the network path between a represented host device and the shared resource has changed, instances of spoofing may be detected.

During the telephone conference, the Examiner explained that he believed the above quoted language could be interpreted several ways. In particular, the Examiner asserted that it was not clear what a “physical connection through the network” refers to such that the scope of the claims is ambiguous. While Applicant disagrees, the claims containing the same or similar language have been amended, particularly pointing out what is meant by a physical connection through the network. Specifically, each of the independent claims has been amended to recite “at least one network component” connected to the network, wherein the physical connection is recited as the “port of the at least one network component” at which the respective device is connected.” Applicant believes the amendments to the claims unambiguously describe with specificity the physical connection through the network.

Thus, claim 1, as amended, recites that the network assigns a second identifier to each of the plurality of devices, “the second identifier indicating a port of at least one network component through which the respective device accesses the network.” Claim 1 further recites “determining whether the one of the plurality of devices is attempting to access the shared resource through a port of the at least one network component that is different than a first port of the at least one network component used by the first device to access the shared resource using the second identifier.”

Claim 23, as amended, recites “a second identifier that uniquely identifies a port of at least one network component through which the respective device accesses the network.” Claim 23 further recites “determining whether the one of the plurality of devices is attempting to login to the

storage system through a port of the at least one network component that is different than a first port of the at least one network component used by the first device to login to the storage system.”

Claim 27, as amended, recites “a second identifier that uniquely identifies a port on at least one network component at which the device is connected, the at least one network component assigning a unique value for the second identifier to each of the plurality of devices that is logged into the network.” Claim 27 further recites “determining whether the one of the plurality of devices is attempting to login to the network through a port on the at least one network component that is different than a first port of the at least one network component through which the first device previously logged into the network.”

Claim 32, as amended, recites that the network “assigns a second identifier to each of the plurality of devices, the second identifier indicating a port of at least one network component at which the respective device is connected.” Claim 32 further recites determining “whether the one of the plurality of devices is attempting to access the shared resource through a port of the at least one network component that is different than a first port of the at least one network component used by the first device to access the shared resource.”

Claim 57, as amended, recites “a second identifier that uniquely identifies a port on at least one network component through which the respective device connects to the network.” Claim 57 further recites determining “that the one of the plurality of devices is attempting to access the storage system through a port of the at least one network component that is different than a first port of the at least one network component used by the first device in logging into the storage system when the value of the second identifier presented by the one of the plurality of devices mismatches the stored value of the second identifier for the first device.

Claims 62, as amended, recites “a second identifier that uniquely identifies a port of at least one network component at which the respective device is connected, the at least one network component assigning a unique value for the second identifier to each of the plurality of devices that is logged into the network. Claim 62 further recites determining “whether the one of the plurality of devices is attempting to login to the network through a port that is different than a first port of the at least one network component through which the first device previously logged into the network.”

Thus, each independent claim has been amended to clearly and distinctly point out that the physical connection through the network refers to the port of at least one network component at which the respective device is connected. In addition, corresponding dependent claims have been amended to be consistent with the amendments. Accordingly, the claims 1-66 are believed to satisfy 35 U.S.C. §112 in this respect.

The Office Action also asserts that claims 1-66 are not enabled. This rejection appears to be based on the assertion on pages 7-10 of the Office Action that Applicant's argument that a WWN is insufficient to detect when a physical connection through the network has changed contradicts with the methodology presented in the specification. The Office Action asserts that adopting such a position would appear to render Applicant's description deficient. However, the specification nowhere describes detecting a difference in the physical connection through the network using solely the WWN. Quite the contrary. The specification in fact identifies a security hole resulting from using just the WWN name to authorize access to a shared resource (*see e.g.*, page 18, line 19 – page 19, line 7).

To close this security hole, Applicant describes embodiments where additional information (e.g., a fabric ID) is used in addition to the WWN to detect accesses from different physical connections. Page 19, line 23 – page 20, line 4 state, in relevant part:

In accordance with one illustrative implementation for use in connection with a Fibre Channel fabric, Applicants have appreciated that the fabric ID assigned to a particular HBA is, in practice, an indication of the physical port that provides the window into the fabric for that HBA...Switch manufacturers use an assignment technique that is consistent, such that each port is always assigned the same fabric ID. As a result, the fabric ID assigned to an HBA actually identifies a physical relationship between the HBA and the port of the fabric switch that provides the window into the fabric 206 (FIG. 2) for that HBA.

The specification then proceeds to describe one embodiment where the WWN and fabric ID may be used together to determine if a represented device is attempting to access a shared resource from a different physical connection through a network switch. In particular, page 20 line 32 – page 21, line 10 state:

When an HBA attempts to login to the storage system 20, the HBA must provide both its WWN and its fabric ID to the storage system 20. Upon receiving the WWN and the fabric ID, the filter and adapter unit 34 performs a search of the master filter table 276, to determine whether there is an existing entry corresponding to the WWN of the HBA attempting to login to the storage system. If such an entry exists, the filter and adapted unit 34 compares the fabric ID for the HBA in the corresponding entry in the table 276 with the fabric ID for the HBA attempting to login to the storage system, and if these fabric IDs do not match, the filter and adapter unit 34 prevents the requesting HBA from logging into the storage system, and if these fabric IDs do not match, the filter and adapter unit 34 prevents the requesting HBA from logging into the storage system 20.

Accordingly, Applicant's argument that a WWN name is insufficient by itself to detect changes in a physical connection through the network fully comports with Applicant's specification and claims. Nowhere does the specification describe making determinations about a host devices physical connection through the network using solely the WWN as asserted in the Office Action, and the specification fully supports the claims as currently presented. Accordingly, Applicant respectfully requests that the rejection of the claims under 35 U.S.C. §112 be withdrawn.

The foregoing description of some embodiments is provided solely to illustrate that the specification nowhere describes using the WWN alone to determine information about the physical connection of a particular device through the network, and to show that embodiments described therein provide support for and enable the claims. It should be appreciated that each of the independent claims may not be limited in the manner described in the exemplary embodiments discussed above.

II. Rejections Under 35 U.S.C. §102

The Office Action rejects claims 1-66 under 35 U.S.C. 102(e) as purportedly being anticipated by US Patent No. 6,343,324 (Hubis). While Applicant believes the claims as previously presented distinguish over Hubis, Applicant has amended claims 1-5, 9, 10, 13, 14, 17, 20, 23, 24, 27, 30, 32-36, 40, 41, 44-46, 48, 51, 54-58, 61, 62, 65 and 66 to clearly point out the distinctions. In particular, each independent claim has been amended in view of the Examiner's assertion that the language "physical connection through the network" could allegedly be interpreted such that Hubis reads on the claims. The claims have been amended with increased specificity with respect to the

above quoted language to clearly distinguish over Hubis. Provided below is an overview of embodiments of Applicant's invention and a detailed discussion of Hubis to assist in clarifying the pertinent differences.

A. Overview of Embodiments of the Invention

During the telephone conference, Applicant's representatives discussed a data management technique for preventing certain types of malicious access to a shared resource, described in Applicant's specification, that could not be prevented using conventional authorization schemes, and more particularly, the authorization scheme described in Hubis. In particular, beginning at page 18, line 3 of the Specification, Applicant identifies that in networked environments where hosts accessing a common storage system may not trust each other, conventional authorizing schemes may be insufficient to guard against inadvertent and/or malicious access to another host device's storage locations (*see e.g.*, page 18, lines 3-18 of the Specification). One example of malicious access that conventional authorization security measures may fail to guard against is spoofing, where a host device attempts to take over the identity of another device on the network to bypass the security measures and access storage locations allocated to another (*see e.g.*, page 18, lines 19-23 of the Specification).

Applicant describes one example of spoofing in the context of a Fibre Channel environment where security mechanisms to prevent unauthorized access to storage locations are keyed on the WWN name of host devices accessing the common storage system. This example is particularly germane to the outstanding rejection as it closely describes the environment described in Hubis, as discussed in further detail below. The Fibre Channel protocol enables host devices logged on to the Fibre channel fabric to issue a command requesting identification of the WWNs of all other host devices on the network (*see e.g.*, page 18, lines 24-27 of the Specification). The Fibre Channel protocol also enables a host device to set its own WWN (*see e.g.*, page 18, lines 31-32 of the Specification). Accordingly, by issuing the appropriate request, a malicious host device can obtain another device's WWN and use it as its own when requesting access to a shared storage system. Thus, conventional security mechanisms that authorize access by keying the WWN are vulnerable to these types of attack (*see e.g.*, page 18, line 27 – page 19, line 7 of the Specification).

In some embodiments, Applicant has addressed the problem by ensuring that, when a host device presents a unique identifier (e.g., a WWN) to access the data storage, the host device is accessing the data storage through the same physical connection through the network from which it previously accessed the storage device (*see e.g.*, page 19, lines 7-13 of the Specification). By detecting when a host device is attempting to access the data storage through a different path through the network, spoofing devices can be detected and denied access to the data storage (*see e.g.*, page 19, lines 13-17 of the Specification). In some embodiments, the fabric identification (fabric ID) of a host device may be used to detect when a host device is attempting to access the data storage through a different physical connection path through the Fibre Channel fabric (*see e.g.*, page 19, lines 23-26 of the Specification).

Since the fabric ID is assigned to host devices by the fabric switch, a host device cannot select its own fabric ID and therefore cannot appropriate the fabric ID of another. Moreover, since the fabric ID is assigned based on the port through which the host device is accessing the network, the fabric ID identifies the physical relationship between the host device and the fabric switch, and may be used as an indicator of the physical connection through the network used to access the storage device (see *e.g.*, page 19, line 23 – page 20, line 2 of the Specification). In particular, the fabric ID may be used to identify the physical connection path used by the host device through the fabric switch (*see e.g.*, page 20, lines 2-4 of the Specification).

Applicant appreciated that using an identifier that indicates something about the physical configuration of the host device with respect to the network may facilitate safeguarding against malicious host devices. For example, in some embodiments, the WWN may be used in connection with the fabric ID to detect when a host device representing itself as a another device via a presented WWN is attempting to access the data storage through a different physical connection through the fabric switch. For example, when a host device first accesses the storage device, the WWN and fabric ID of the device may be stored. Subsequently, any device attempting to access the storage device using the same WWN must also have the same fabric ID, or else access to the storage device is denied (*see e.g.*, page 20, line 32 – page 21, line 10 of the Specification). Data management techniques that check to make sure that host devices access the network through the

same port of a network component, such as a fabric switch, before permitting data access are entirely missing from Hubis, as discussed in further detail below.

The foregoing summary is provided solely for the convenience of the Examiner. It should be appreciated that each of the independent claims may not be limited in the manner described in the summary above. Therefore, the Examiner is requested not to rely upon the summary for determining whether each of the claims distinguishes over the prior art of record, but to do so based solely on the language of the claims themselves and the arguments presented below.

B. US Patent No. 6,343,324 (Hubis)

Hubis describes a system for controlling access to a shared storage device using a Host-to-Volume Mapping (HVM) that restricts access to logical volumes to a single host or group of hosts (col. 5, lines 12-15). As discussed during the telephone conference, Hubis restricts access to logical volumes based upon the WWN presented by a host device attempting to access logical volumes of the storage device. In particular, whether a device is allowed access to a logical volume depends on whether the WWN presented by the device is listed in the Volume WWN table 130 for the requested volume, as shown in FIG. 2B-2 and described in column 11, lines 45-47.

Accordingly, Hubis' authorization process is keyed to the presented WWN. No other check is made to determine whether the host device's request should be accepted or denied, and no mechanism exists in Hubis to prevent a device from using a false WWN to access the storage device from another location on the network. Hubis nowhere mentions spoofing as a security threat, or even recognizes that malicious devices may present the WWN of another device to gain access to the storage device. In fact, Hubis describes an authorization scheme that would actually permit malicious devices spoofing another host device to successfully access logical volumes allocated to another.

In the Response to the Office Action mailed on October 5, 2004 (Previous Response), Applicant described in detail how the authorization process of Hubis would react to a device attempting to access logical volumes of another device by spoofing the identity of the other device, by precisely following the flow chart diagrams of FIGS. 3a and 3b and the accompanying description at column 14, line 41 – column 15, line 9 of Hubis. Because Hubis nowhere determines whether a host representing itself as a specific host (e.g., via a WWN) is attempting to access the

storage device through a same or different port of at least one network component, a device spoofing the identity of another will successfully access the requested logical volumes. In particular, because only the WWN is checked, a spoofing device will correctly establish an entry for itself in the Host ID Map 155 regardless of how the device is connecting to the storage device (Applicant respectfully refers the Examiner to the Previous Response for a more detailed description of Hubis' HVM structure and the operation of the authorization scheme described in Hubis).

Hubis nowhere discusses any mechanism for preventing multiple entries in the Host ID Map from being established, such as by a host using the same WWN from different physical locations on the network. Hubis simply lacks any disclosure relating to ensuring that hosts do not spoof their identity. In particular, Hubis is completely silent with respect to determining whether hosts that represent themselves with the same identity are attempting to access the storage device over different physical connections, and more particularly, through a different port of a network component connected to the network through which the device is attempting to access the storage device.

Claim 1 recites a method for use in a computer system including a plurality of devices each having a first identifier that uniquely identifies the respective device, a shared resource shared by the plurality of devices, and a network that couples the plurality of devices to the shared resource, the network including at least one network component adapted to assign a second identifier to each of the plurality of devices, the second identifier indicating a port of at least one network component through which the respective device accesses the network. The method includes “determining whether the one of the plurality of devices is attempting to access the shared resource through a port of the at least one network component that is different than a first port of the at least one network component used by the first device to access the shared resource using the second identifier,” which is nowhere disclosed or suggested in Hubis. Therefore, claim 1 patentably distinguishes over Hubis and is in allowable condition.

Claims 1-22 depend from claim 1 and are allowable based at least upon their dependency.

Claim 23 recites a method for use in a computer system including a plurality of devices, a storage system shared by the plurality of devices, and a network that couples the plurality of devices to the storage system, wherein the network employs a protocol wherein each of the plurality of

devices has a first identifier that uniquely identifies the device in a manner that is independent of a physical configuration of the computer system and a second identifier that uniquely identifies a port on at least one network component at which the device is connected. The method includes “determining whether the one of the plurality of devices is attempting to login to the storage system through a port of the at least one network component that is different than a first port of the at least one network component used by the first device to login to the storage system,” which is nowhere disclosed or suggested in Hubis. Therefore, claim 23 patentably distinguishes over Hubis and is in allowable condition.

Claims 24-26 depend from claim 23 and are patentable based at least upon their dependency.

Claim 27 recites a method for use in a computer system including a network and a plurality of devices coupled to the network, the network employing a protocol wherein each of the plurality of devices has a first identifier that uniquely identifies the device in a manner that is independent of a physical configuration of the computer system and a second identifier that uniquely identifies a port on at least one network component at which the device is connected, the at least one network component assigning a unique value for the second identifier to each of the plurality of devices that is logged into the network. The method includes “determining whether the one of the plurality of devices is attempting to login to the network through a port on the at least one network component that is different than a first port of the at least one network component through which the first device previously logged into the network,” which is nowhere disclosed or suggested in Hubis. Therefore, claim 27 patentably distinguishes over Hubis and is in allowable condition.

Claims 28-31 depend from claim 27 and are patentable based at least upon their dependency.

Claim 32 recites an apparatus for use in a computer system including a plurality of devices, a shared resource shared by the plurality of devices each having a first identifier that uniquely identifies the respective device, and a network that couples the plurality of devices to the shared resource, the network including at least one network component adapted to assign a second identifier to each of the plurality of devices, the second identifier indicating a port of at least one network component at which the respective device is connected. The apparatus includes at least one controller to “determine whether the one of the plurality of devices is attempting to access the shared resource through a port of the at least one network component that is different than a first

port of the at least one network component used by the first device to access the shared resource,” which is nowhere disclosed or suggested in Hubis. Therefore, claim 32 patentably distinguishes over Hubis and is in allowable condition.

Claims 32-56 depend from claim 32 and are patentable based at least upon their dependency.

Claim 57 recites an apparatus for use in a computer system including a plurality of devices, a storage system shared by the plurality of devices, and a network that couples the plurality of devices to the storage system, wherein the network employs a protocol wherein each of the plurality of devices has a first identifier that uniquely identifies the device in a manner that is independent of a physical configuration of the computer system and a second identifier that uniquely identifies a port on at least one network component through which the respective device connects to the network. The apparatus comprises at least one controller to “determine that the one of the plurality of devices is attempting to access the storage system through a port of the at least one network component that is different than a first port of the at least one network component used by the first device in logging into the storage system when the value of the second identifier presented by the one of the plurality of devices mismatches the stored value of the second identifier for the first device,” which is nowhere disclosed or suggested in Hubis. Therefore, claim 57 patentably distinguishes over Hubis and is in allowable condition.

Claims 58-61 depend from claim 57 and are patentable based at least upon their dependency.

Claim 62 recites an apparatus for use in a computer system including a network and a plurality of devices coupled to the network, the network employing a protocol wherein each of the plurality of devices has a first identifier that uniquely identifies the device in a manner that is independent of a physical configuration of the computer system and a second identifier that uniquely identifies a port of at least one network component at which the respective device is connected, the at least one network component assigning a unique value for the second identifier to each of the plurality of devices that is logged into the network. The apparatus comprises at least one controller “to determine whether the one of the plurality of devices is attempting to login to the network through a port that is different than a first port of the at least one network component through which the first device previously logged into the network, and to deny the attempted login by the one of the plurality of devices to the network when the one of the plurality of devices is

attempting to login to the network through a port of the at least one network component that is different than the first port,” which is nowhere disclosed or suggested in Hubis. Therefore, claim 62 patentably distinguishes over Hubis and is in allowable condition.

Claims 63-66 depend from claim 62 and are patentable based at least upon their dependency.

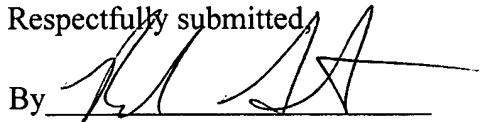
CONCLUSION

A Notice of Allowance is respectfully requested. The Examiner is requested to call the undersigned at the telephone number listed below if this communication does not place the case in condition for allowance.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Dated: December 26, 2006

Respectfully submitted,

By 

Richard F. Giunta

Registration No.: 36,149

WOLF, GREENFIELD & SACKS, P.C.

Federal Reserve Plaza

600 Atlantic Avenue

Boston, Massachusetts 02210-2206

(617) 646-8000